UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,812	11/29/2005	Christophe Justin Evrard	550-619	4576

23117   7590   01/17/2007
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER
VICARY, KEITH E

ART UNIT	PAPER NUMBER
2196	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

	Application No.	Applicant(s)
Office Action Summary	10/527,812	EVRARD ET AL.
	Examiner	Art Unit	
	Keith Vicary	2196	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2005*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 March 2005* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date *3/14/2005*.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____ .

DETAILED ACTION

1.   The Notice of Noncompliant Amendment previously filed on 12/20/06 is

withdrawn.

2.   Claims 1-10 are pending in this application. Claims 3 and 8 are amended by an

amendment filed on 3/14/2005. Claims 1-10 are presented for examination.

Specification

3.   The following guidelines illustrate the preferred layout for the specification of a
utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should
include the following sections in order. Each of the lettered items should appear in
upper case, without underlining or bold type, as a section heading. If no text follows the
section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR
        DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A
        COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
        (1) Field of the Invention.
        (2) Description of Related Art including information disclosed under 37
        CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A
        "Sequence Listing" is required on paper if the application discloses a
        nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if

the required "Sequence Listing" is not submitted as an electronic
document on compact disc).

The specification is objected to for failing to include the above section headings

where necessary. Appropriate correction is required.

4.   The disclosure is objected to because of the following informalities. Appropriate

correction is required.

a.   There is a closed parenthesis without a corresponding open parenthesis

on page 11, line 24.

b.   "Figure 13" on page 13, line 25 should be "Figure 12."

Drawings

5.   The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5)

because they include the following reference character(s) not mentioned in the

description: **144** of Figure 14 (this label should be explicitly referred to somewhere in

page 14, last paragraph) and label **28** in Figure 13 should be labeled as **128.** Corrected

drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification

to add the reference character(s) in the description in compliance with 37 CFR 1.121(b)

are required in reply to the Office action to avoid abandonment of the application. Any

amended replacement drawing sheet should include all of the figures appearing on the

immediate prior version of the sheet, even if only one figure is being amended. Each

drawing sheet submitted after the filing date of an application must be labeled in the top

margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If

the changes are not accepted by the examiner, the applicant will be notified and

informed of any required corrective action in the next Office action. The objection to the

drawings will not be held in abeyance.

Claim Objections

6.   Claim 10 is objected to because of lack of antecedent basis. Appropriate

correction is required.

        c.   "dummy register," claim 10, line 1, is being read as "trash register" for the

purposes of this office action.

Claim Rejections - 35 USC § 102

7.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8.   Claims 1-2, 5-7, and 10 are rejected under 35 U.S.C. 102(e) as being anticipated

by Qiu et al. (Qiu) (US 6804782 B1).

        Consider claim 1, Qiu discloses an apparatus for processing data,

comprising a process core (col. 4, lines 54-55) operable to execute data

processing instructions to generate result data values (col. 3, lines 24-28;

mathematical operations); and

data processing registers holding data values defining state of said

processor core to which said result data values are written (col. 7, lines 19-21,

37, 40-48); wherein

at least one data processing instruction executed by said processor core

is a conditional write data processing instruction (col. 3, lines 50-56 and col. 4,

lines 1-5; the multiplication operations and storing the result are conditional

based on the private key) encoding condition codes specifying conditions under

which said conditional write data processing instruction will or will not be

permitted to write data to effect a change in state of said processor core (col. 4,

lines 23-32 and 61-63, col. 5, lines 22-32; the cryptographic key determines the

conditions under which the multiplication operation is emulated or not): and

further comprising

a trash register to which a result data value may be written instead of a

data processing register upon execution of said conditional write data processing

instruction when said condition codes within said conditional write data

processing instruction do not permit a write to effect a change in state of said

processor core (col. 3, lines 28-31 and 61-65, col. 4, lines 1-11, 23-35 and col. 5,

lines 37-47; the second memory correlates to the trash register).

Consider claim 6, Qiu discloses a method of processing data, comprising generating result data values upon execution by a processor core of data processing instructions (col. 4, lines 54-55, and col. 3, lines 24-28; mathematical operations), at least one data processing instruction executed being a conditional write data processing instruction (col. 3, lines 50-56 and col. 4, lines 1-5; the multiplication operations and storing the result are conditional based on the private key) encoding condition codes specifying conditions under which said conditional write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core (col. 4, lines 23-32 and 61-63, col. 5, lines 22-32; the cryptographic key determines the conditions under which the multiplication operation is emulated or not) and wherein

a result data value is not written to a data-processing register holding a data value defining state of said processor core (col. 7, lines 19-21, 37, 40-48); when condition codes within said condition write data processing instruction do not permit a write to effect a change in state of said processor core but is instead written to a trash register (col. 3, lines 28-31 and 61-65, col. 4, lines 1-11, 23-35 and col. 5, lines 37-47; the second memory correlates to the trash register).

Consider claims 2 and 7, Qiu discloses said data processing register is part of a register bank having a plurality of data registers to which result data values are written (col. 5, lines 37-47; together the first memory and the second memory make up one bank in the same overall location as in Figure 4; also note

that as in claims 1 and 6 above, the later mentioned registers are one

embodiment of these memories).

Consider claims 5 and 10, Qiu discloses said trash register is part of said

register bank (col. 5, lines 37-47; together the first memory and the second

memory make up one bank in the same overall location as in Figure 4), said

trash register being unmapped to a register number such that said trash register

may not be specified by a register specifying operand value (col. 5, lines 37-47;

given that the second memory is used exclusively for when unnecessary stores

to memory are required, and an unnecessary store is only deemed unnecessary

based on the cryptographic key, and not based on any arguments/parameters in

the instruction, it is inherent that the second memory cannot be specifically

specified as an operand. Furthermore, in col. 7, lines 21-23 and 43-45, the

unnecessary store is stored in a temporary register, which is well-known in the

art to mean a register which is not user-addressable but is instead used for

intermediate calculations).

Claim Rejections - 35 USC § 103

9.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

10.   Claims 3-4 and 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Qiu as applied to claims 1 and 6 above, and further in view of Kissell (US 6625737

B1).

Consider claims 3 and 8, Qiu does not explicitly disclose that writing to

said trash register is programmably disabled by a trash register control signal,

although he does state that the total number of emulated operations, and thus

the number of write operations to the second memory, can be controlled (col. 1,

lines 52-54).

Although it would have been obvious to disable unnecessary storing by

using a simple control signal, Kissell nevertheless discloses that writing to said

trash register is programmably disabled by a trash register control signal (col. 8,

lines 10-23, 41-46; the inhibit/burn signal line controls the power consumption of

the processor by turning on/off subsystems, analogous to how the trash register

control signal would turn on/off the multiplication/storing subsystem).

The teaching of Kissel fits into the environment of Qiu as both deal with

consuming extra power to mask attempts of differential power analysis.

Therefore, it would have been obvious to one of ordinary skill in the art at

the time of the invention to combine the teaching of Kissel with the invention of

Qiu in order to selectively control the operation of the invention in case it is not

necessary.

Consider claims 4 and 9, Qiu does not explicitly disclose that said trash register control signal is stored in a system configuration register.

Although it would have been obvious to store a signal that affects the operation of a processor in a system configuration register (such as an interrupt enable flag in a program status word register), Kissel nevertheless discloses that said trash register control signal is stored in a system configuration register (col. 8, lines 10-23; the maximum power threshold register essentially determines the value of the inhibit/burn signal).

The teaching of Kissel fits into the environment of Qiu as both deal with consuming extra power to mask attempts of differential power analysis.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teaching of Kissel with the invention of Qiu in order to selectively control the operation of the invention with good response time, as storing an operational parameter in a register takes less time to retrieve than storing in a memory.
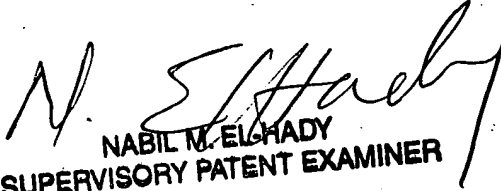
Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Keith Vicary whose telephone number is (571) 270-1314. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nabil El-Hady can be reached on 571-272-3963. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KV
KV

NABIL M. EL-HADY
SUPERVISORY PATENT EXAMINER